UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/805,279	03/13/2001	Robert M. Barnhart	SAIC0039	1264

27510 7590 01/11/2005

KILPATRICK STOCKTON LLP
607 14TH STREET, N.W.
WASHINGTON, DC 20005

EXAMINER	
JARRETT, SCOTT L	

ART UNIT	PAPER NUMBER
3623	

DATE MAILED: 01/11/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/805,279	BARNHART, ROBERT M.	
	Examiner	Art Unit	
	Scott L. Jarrett	3623	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 March 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Objections

1. Claims 5, 13, 19, 24 and 27 objected to because of the following informalities. Appropriate correction is required.

Regarding Claim 24, claim 24 intended to claim "cast more than one" instead of the "cat more than one" as disclosed. .

Regarding Claims 5, 13, 19 and 27 the claim language "allowing the individual" would more clearly describe the system providing for the verification/confirmation of a vote by a voter if the claims were amended to read verification of a vote by a voter. Examiner suggest applicant amend the claims.

Claim Rejections - 35 USC § 101

2. Claims 1-14 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

The basis of this rejection is set forth in a two-prong test of:

(1) whether the invention is within the technological arts; and

(2) whether the invention produces a useful, concrete, and tangible result.

For a claimed invention to be statutory, the claimed invention must be within the technological arts. Mere ideas in the abstract (i.e., abstract idea, law of nature, natural phenomena) that do not apply, involve, use, or advance the technological arts fail to

promote the "progress of science and the useful arts" (i.e., the physical sciences as opposed to social sciences, for example) and therefore are found to be non-statutory subject matter. For a process claim to pass muster, the recited process must somehow apply, involve, use, or advance the technological arts.

Regarding Claims 1-14, claims 1-14 only recite an abstract idea. The recited method for securely voting over a network does not apply, involve, or use the technological arts since all of the recited steps can be performed in the mind of the user or by use of a pencil and paper. The claimed invention, as a whole, is not within the technological art as explained above claims 1-14 are deemed to be directed to non-statutory subject matter.

As to technological arts recited in the preamble, mere recitation in the preamble (i.e., intended or field of use) or mere implication of employing a machine or article of manufacture to perform some or all of the recited steps does not confer statutory subject matter to an otherwise abstract idea unless there is positive recitation in the claim as a whole to breathe life and meaning into the preamble. In the present case, none of the recited steps are directed to anything in the technological arts as explained above with the exception of the recitation that the method involves a “network”, a “server” and a “digital signature.” Looking at the claims as a whole, nothing in the body of the claims recites any structure or functionality to suggest that a computer performs the recited steps. Therefore, the terms discussed are taken to merely recite a field of use and/or nominal recitation of technology.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-6, 10-19 and 24-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Karro et al., Towards a Practical, Secure and Very Large Scale Online Election (1999).

Regarding Claims 1 and 15 Karro et al. teach the significant research, development and interest in electronic voting over computer networks (Introduction, Paragraph 3, Page 1). Karro et al. further teach the plurality of systems, methods and techniques for electronic voting systems (Introduction, Pages 1-2; Bibliography, Pages 8-9).

More specifically Karro et al. teach a system for securely voting over a network (online; Abstract, Page 1), comprising:

- six components/sub-systems: registrar, authenticator, matcher, distributor, verifier and counter (Section 4 The proposed protocol, Pages 4-5; Figures 1-3 Pages 4-5 and as shown below);

- delivering an electronic ballot from a server with a ballot identification number (vote serial number, ballot ID, b_ID; as shown in Figure 3 below; Pre-Voting Phase, Step 2, Page 4; Voting Phase Steps 1-4, Page 5);

- completing, digitally signing and submitting the ballot (Voting Phase Step 5, Page 5) and the ballot identification number; and

- creating of a plurality of data elements (records, stores, etc.) including but not limited to the ballot, voter ID, election choices, ballot ID, election ID, etc. (Voting Phase Step 5, Page 5; Section 5.1 Data Protection, Page 6; Figure 1, ID/Key DB, Page 4; Figures 1-3, Pages 4-5 and as shown below).

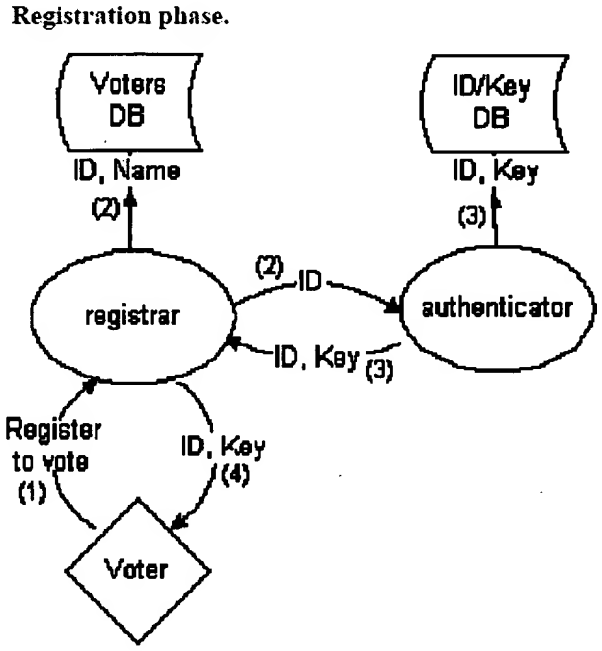

Figure 1: Registration Phase

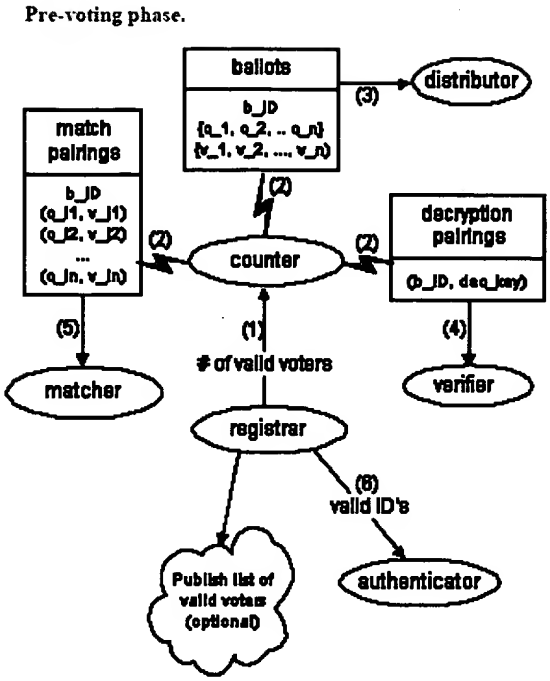

Figure 2: Pre-voting stage

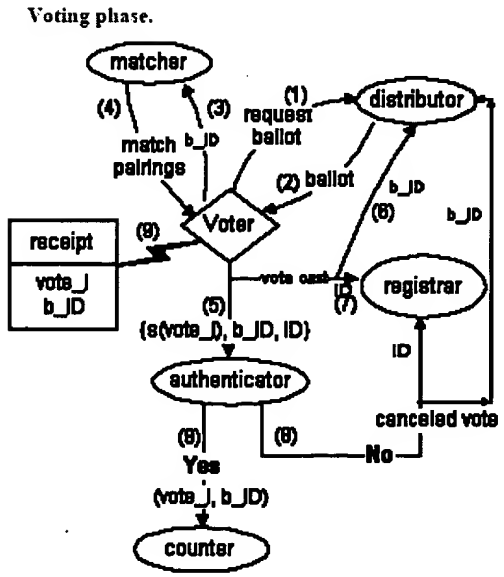

Figure 3: Voting Stage

Regarding Claims 2, 5, 16 and 19 Karro et al. teach the confirmation of the vote's receipt and retention by the system to the voter. More specifically Karro et al. teaches communication with the voter if there is discovered to be an issue with the submitted vote as well as the transmission of a receipt confirming the vote's submission (Voting Phase, Steps 8-9, Page 5; Figure 3, Page 5 and as shown below).

Karro et al. further teach that the system for securely voting over a network further comprises:

- a minimum of two sub-systems the authenticator and the counter that publish the encrypted ballots and ballot ID numbers (Announcement Phase, Page 5);

- the voters ability to change his/her vote (Column 1, Page 8);

- the verification and confirmation of a vote by a voter (allowing the voter to decompose his/her vote; Announcement Phase, Page 5; Lemmas 3 and 5, Page 7); and

- the verification of the vote by the verification sub-system (Announcement Phase, Page).

Karro et al. does not expressly teach that the confirmation (receipt) is signed or that the ballot contains all the information as claimed.

Official notice is taken that the signing of a communication (receipt) as a means for certifying the authenticity of the communication or insuring the privacy of the communication is old and very well known in the art and that the decision to sign the

entire contents of the voting record as part of the confirmation is an obvious design choice. Further sending the entire contents of the voting record to the voter is an obvious means for enabling the user to keep a complete copy of his/her voting record.

In the Karro et al. invention the publishing of the complete voting record online increases the verifiable of the election as well as reduces the time and costs associated with sending the complete voting record to each voter whether they want the record or not.

It would have been obvious to one skilled in the art at the time of the invention that the system for securely voting over a network as taught by Karro et al. would have benefited from enabling voters to receive their complete voting record as part of the vote confirmation process thereby insuring a voter's ability to save a copy of their complete voting record.

Regarding Claims 3-4 and 17-18 Karro et al. teach a variety of systems and methods for insuring the integrity and accuracy of an election. More specifically Karro et al. teach the use of the voter as discussed above as well as the authenticator, distributor, counter and verification sub-systems to insure the ballots have been cast, not tampered with and are accurately counted (Section 4 The proposed protocol, Pages 4-5; Lemmas 2, 3 and 5, Page 7; Column 2, Page 8; Figure 3, Page 5 and as shown above).

Karro et al. further teach the reconstruction of a ballot as a means for insuring the vote has not been tampered with as discussed above.

Regarding Claim 6 Karro et al. teach the storage of the voter's encryption key on a portable storage device and reading the device prior to voting (floppy disk; Column 2, Page 4).

Regarding Claim 10 Karro et al. teach that the accuracy of an election depends on its ability to process/handle three types of votes invalid (ineligible voters), votes made by eligible voters but in incorrect formats and votes generated for unused ballots (Lemma 3, page 7). Karro et al. further teach the detection of attempts to cast more than one ballot by the distributor, authenticator and registrar sub-systems (Voting Phase, Steps 6-7, Page 5; Announcement Phase, Page 5; Lemma 2, Page 7).

Regarding Claims 11 and 25 Karro et al. does not teach rendering the ballot as a bit map.

Official notice is taken that the representation (display, presentation, etc.) of a document as an image (bitmap, JPEG, GIF, etc.) is old and very well known in the art. Further it is well known in the art that corrupting (defrauding, manipulating) an image is more difficult than corrupting plain text and therefore provides an additional level of security.

It would have been obvious to one skilled in the art at the time of the invention that the system for secure voting over a network as taught by Karro et al. would have benefited from the use of a plurality of well known document representation techniques, technologies or methods including but not limited to the representation of a document as an image.

Further it would have been obvious to one skilled in the art at the time of the invention that the system for secure voting over a network as taught by Karro et al. would have benefited from the additional security that utilizing an image instead of plaintext for presenting and storing a ballot would have provided.

Regarding Claims 12 and 26 Karro et al. teach an online election system as discussed above. More specifically Karro et al. teach the presentation of ballots to voters utilizing Internet browsers (Netscape; Section 4 The proposed protocol, Page 4; Voting Phase, Page 5); the definition of an Internet browser being an application used for displaying HTML documents, and other WWW documents.

Regarding Claim 13, claim 13 recites similar limitations to Claims 1, 2 and 5 and is therefore rejected using the same art and rationale as applied in the rejection of Claims 1, 2 and 5.

Regarding Claim 14, claim 14 recites similar limitations to Claims 1, 3, and 4 and is therefore rejected using the same art and rationale as applied in the rejection of Claims 1, 3, and 4.

Regarding Claim 24 Karro et al. teach a plurality of means for insuring an individual does not cast more than one vote as discussed above.

Karro et al. does not teach the use of a one-way hash function as a means for identifying individuals who attempt to cast more than one vote.

Official notice is taken that one-way hash functions are widely used for data integrity in conjunction with digital signature schemes and that cryptographic hash functions generate a hash-value which serves as a compact representative image (sometimes called an imprint, digital fingerprint, or message digest) of an input string, and can be used as if it were uniquely identifiable with that string therefore providing a simple means for identifying identical records (attempts of individuals to cast more than one vote).

It would have been obvious to one skilled in the art at the time of the invention that the system for securely voting over a network as taught by Karro et al. would have benefited from the additional security and accuracy provided by the use of one-way

hash functions as a means for identifying individuals who attempt to cast more than one vote (duplicate records).

Regarding Claim 27, claim 27 recites similar limitations to Claims 1, 2, and 5 and is therefore rejected using the same art and rationale as applied in the rejection of Claims 1, 2, and 5.

Regarding Claim 28, claim 28 recites similar limitations to Claims 1 and 4 and is therefore rejected using the same art and rationale as applied in the rejection of Claims 1 and 4.

5. Claim 7-8 and 20-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Karro et al., Towards a Practical, Secure and Very Large Scale Online Election (1999) as applied to claims 1-6, 10-19 and 24-28 above and further in view of London Shrader et al., U.S. Patent Publication No. 2002/007887.

Regarding Claims 7-8 and 20-21 Karro et al. teach an online system for securely voting over a network further comprising the storage pf the voter's encryption key on a portable storage device for access prior to voting as discussed above.

Karro et al. does not expressly teach the storage of additional information on a portable storage device, the use of a smart card or the use of certificates.

London Shrader et al. teach a system for secure voting over a network further comprising a plurality of user authentication and data encryption schemes including but not limited to:

- public/private key encryption systems and methods (Paragraph 0034, page 3; Paragraphs 0048-0050, Pages 4 and 5);

- digital certificates and certificate authorities (Paragraph 0017, Page 2; Paragraphs 0052---53, Page 5);

- Light-weight Directory Application Protocol (LDAP; Paragraphs 0052-0053, Page 5; Paragraph 0060, Page 5); and

- hash functions (Paragraph 0061, Pages 5-6).

London Shrader et al. further teach the utilization of smart cards as a means for storing and distributing digital certificates (Paragraph 0052, Page 5).

It would have been obvious to one skilled in the art at the time of the invention that the system for securely voting over a network as taught by Karro et al. would have benefited from storage of additional information on a portable storage device, the use of a smart card and the use of digital certificates in view of the teachings of London Shrader et al. thereby improving the overall security of the system and making it possible for voters to securely vote from a plurality of locations.

Regarding Claim 22 Karro et al. does not teach the use of a certificate or that the certificate utilizes the Public-Key Infrastructure (X.509) standard.

Official notice is taken that the Public-Key Infrastructure (X.509) is old, very well known and widely used as a standard for defining digital certificates.

It would have been obvious to one skilled in the art at the time of the invention that the system for securely voting over a network as taught by Karro et al. would have benefited from the use of a well known and accepted standard for creating and managing public-keys (X.509) thereby insuring the ability of the system to utilize the plurality of systems, tools and techniques based on the X.509 standard.

6. Claims 9 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Karro et al., Towards a Practical, Secure and Very Large Scale Online Election (1999), in view of London Shrader et al., U.S. Patent Publication No. 2002/007887 as applied to claims 1-8, 10-22 and 24-28 above, and further in view of Sehr, Richard Peter, U.S. Patent No. 5,875,432.

Regarding Claims 9 and 23 Karro et al. teach a system for securely voting over a network as discussed above.

Karro et al. does not teach the entering of demographic information onto the ballot.

Sehr teaches a secure voting system further comprising the collection of user demographic information (as shown below, Figure3; Figure 7, Element 204; Column 2, Lines 14-17; Claim 1) as a means for assisting in the verification of the identity of the voter (Column 6, Lines 3-14).

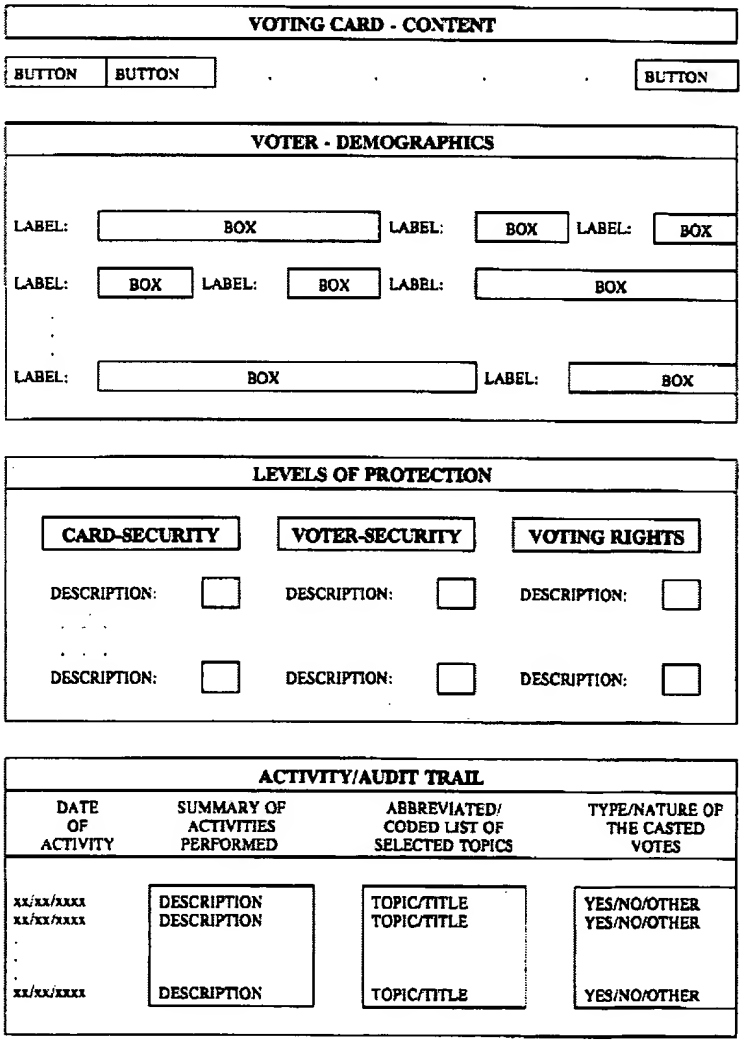

Figure 4: Voter Demographics

It would have been obvious to one skilled in the art at the time of the invention that the system for securely voting over a network as taught by Karro et al. would have benefited from the ability to utilize voter demographic information as an additional security measure thereby assisting in the verification of the identity of the voter in view of the teachings of Sehr.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Drexler et al., U.S. Patent No. 5,412,727, teach a secure electronic voting system utilizing smart cards over a network.

- Brands, Stefanus, U.S. Patent No. 5,521,980, teaches a system for the exchange of certified electronic information over a network further comprising the use of several well-known security techniques including but not limited to digital signatures. Brands further teaches that the system could be used for electronic voting.

- Frankel et al., U.S. Patent No. 6,035,041, teach a system for electronic document signing utilizing public-key encryption.

- Challener et al., U.S. Patent No. 6,081,793, teach a system for secure computer moderated voting.

- Gibbs et al., U.S. Patent No. 6,085,321, teach a system for providing a unique digital signature further comprising the use of a hash function and well-known encryption algorithms.

- Jakobsson, Bjorn Markus, U.S. Patent No. 6,317,883, teaches a secure system for voting over a network further comprising the use of public-private key encryption.

- Davis et al., U.S. Patent No. 6,550,675, teach an automated direct vote recording system further comprising the use of smart cards.

- Sako, Kazue, U.S. Patent Publication No. 2001/0011351, teaches a system for managing anonymous participation in a plurality of electronic activities. Sako further teaches the use of hash functions and other well-known cryptology methods, systems and techniques.

- Jinn-ke et al., A secure electronic voting protocol with IC cards, teaches a system for securely voting over a network further comprising the use of digital signatures, well-known cryptographic authentication techniques and smart cards.

- California Internet Voting Task Force teaches the prevalence and wide-spread research into network based voting systems.

- Herschberg, Mark, Secure Electronic Voting Over the World Wide Web, teaches a system for securely voting over a network further comprising the use of digital signatures, cryptographic authentication and hash functions.

- SafeVote.com, Contra Costa Shadow Election Test, teaches a commercially available system for secure voting over a network further comprising the use of digital signatures, cryptographic authentication and the confirmation of votes.

- Menezes, et al., Handbook of Applied Cryptography, teach applied cryptographic techniques, methods and systems.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Scott L. Jarrett whose telephone number is (703) 306-5679. The examiner can normally be reached on 8:00AM - 5:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hafiz Tariq can be reached on (703) 305-9643. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SJ
1/7/2005

TARIQ R. HAFIZ
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600